AD-A264 014

April 1993/Number 1-93

(2)

security awareness bulletin

Inside:

Department of Defense Security Institute Richmond Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

Staff Writer
Tracy Gulledge

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Security Education and Awareness Team, c/o Defense General Supply Center, 8000 Jefferson Davis Highway, Richmond Virginia 23297-5091; (804) 279-5314, DSN 695-5314. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods as well as through distribution of textual material for direct training application.

Administrative inquiries, new distribution, address changes: please refer as follows:

Army activities: HQ DA (DAMI-CIS), Washington, DC 20310, (202) 695-8920, DSN 225-8920; POC Jim McElroy

Navy & Marine Corps: Security Policy Div (OP-09N), Washington, DC 20350 (202) 433-8858, DSN 288-8858; POC Sue Jones

Air Force: Headquarters AFSPA/SPGB, Kirtland AFB, NM 87117, DSN 246-4787; POC Ken Saxon

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria VA 22314-1651

DISP contractors: Cognizant Security Office

Other government agencies: Headquarters security education office

WOW!!! Something New!!!

COURSE TITLE

Personnel Security Interview Course
(5220.15)

LOCATION

Department of Defense Security Institute
c/o Defense General Supply Center
Richmond, Virginia 23297-5091

LENGTH

Three and One-Half Days

PURPOSE

The *Personnel Security Interview Course* is designed to train and educate DoD personnel who conduct interviews of individuals who perform sensitive duties or work in a security environment.

SCOPE

The *Personnel Security Interview Course* offers training in how to properly conduct a subject interview. Lessons address the purpose of the interview; how to prepare for the interview; the procedures for controlling and conducting interviews; appropriate and inappropriate areas of questioning; effective listening; and how to identify, follow up and resolve issues raised by the interview. The *Personnel Security Interview Course* uses extensive practical exercises, providing students with several opportunities to apply the knowledge and skills taught. Some outside-of-class preparations and problem-solving assignments are required.

PREREQUISITES

This course is for DoD civilian, military or contractor personnel who conduct personnel security interviews. Personnel from other federal agencies are eligible to attend on a space available basis.

ACADEMIC REQUIREMENTS

Regular attendance at and participation in all sessions is required for a certificate of completion.

Don't confuse this course with the Basic Personnel Security Investigations Course (BPSIC). If your employees conduct personnel security investigations, you want BPSIC. But if they conduct pre-investigative interviews to screen personnel, or post-adjudicative interviews to resolve issues, the *Personnel Security Interview Course* is for you.

TRAINING FUNDS A PROBLEM?

If so, it might make sense to host an offering of the *Personnel Security Interview Course* at your location (even overseas). If you provide the facilities, your only cost would be the TDY expenses of 2-3 DoDSI instructors. In addition, we would be willing to tailor the course content and practical exercises to meet your specific needs and your agency's policies. For more information, call DoDSI at DSN 695-4891 or 804-279-4891.

ACQUISITION SYSTEMS PROTECTION

The means by which defense systems and technical data in the acquisitions cycle will be safeguarded from foreign intelligence collection and unauthorized disclosure.

This issue of the *Bulletin* is devoted to defining and exploring the essential purposes and procedures for the Defense Acquisition Systems Protection Program. Although established by DOD Instruction 5000.2 in February 1991, the ASPP still lacks general familiarity and comprehension within the security community. It is in fact *an application of the information security program* designed to protect essential information, which may or may not be formally classified, with a special focus on weapons systems during their acquisition phases or life cycle. And what exactly, as was asked by this editor, is the acquisition life cycle? It is principally the entire span of time from the first conception of a system to its delivery or fielding—including research, engineering, manufacturing, and testing. But it doesn't end with the system's delivery to the end-user, because (as described by Dr. Elliff in the interview which follows) a good protection plan will include built-in protection safeguards that will protect the integrity of the system should it fall into enemy hands.

The end objective, of course, is to safeguard the technological superiority of our weapons systems in combat—to ensure that if and when a weapon system is used, it won't be met with countermeasures that diminish or neutralize its effectiveness. How do we do this: By denying potential adversaries access to critical technologies and information from the very start of the acquisition process.

We hope that you will find the articles in this issue helpful. DODSI's Cynthia Kloss provides a simple illustration of the ASP concept for most of us who find this idea to be entirely new. And our new Director of Security Programs, Dr. John Elliff, offers a great deal of insight into the process of identifying just what information we must protect. And as Dr. Elliff points out, we don't select information for protection just by intuition or common sense. Critical decisions like these are to be based on solid information about the foreign intelligence threat and the importance of the technology. This underscores, once again, the dependency of security professionals on our national and military intelligence and counterintelligence organizations for current and authoritative threat information.

But what about the threat? Hasn't the demise of the monolithic Soviet Bloc made additional security safeguards superfluous? *Not!* In a recent article about acquisition systems protection in *Program Manager*, reprinted here, author Edward P. Casey states the case for the ASPP being *more*, not *less*, essential as a result of the end of the Cold War. According to Casey, while we are no longer confronted by the KGB and its surrogates, in the post-Cold War world, we are faced by a growing number of intelligence agencies of our allies and former enemies who will use their collection assets to pursue what they perceive as their legitimate national interest.

Lastly, we should not fail to point out the relationship between the Acquisition Systems Protection Program and OPSEC. [see the SAB for March 1992, #3-92] Some people have declared the ASPP to be OPSEC for industry. This is misleading because government as well as industry is involved and the ASPP is a cross-discipline approach. For example, classification management is also a key part of the ASPP: Discrete elements of information which serve an adversarial interest must be identified. As security resources decrease, we must focus protection on those aspects of a system that truly require expenditure of limited funds and personnel.

Questions and Answers about
Acquisition Systems Protection

John T. Elliff

Director, Defense Security Programs Office of the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures)

We take this opportunity to introduce our readership to John T. Elliff who assumed the duties of Director for Defense Security Programs this past August, after the retirement of Art Fajans. Dr. Elliff served on the staff of the Senate Select Committee on Intelligence from 1977 to 1992 where he was responsible for budget authorization review of counterintelligence and security programs and for general oversight of the intelligence community. After receiving a Ph.D. in political science from Harvard in 1968 he taught at Barnard College and later at Brandeis University. He is the author of books on the Justice Department and the FBI.

In this interview Dr. Elliff provides the reader with a general overview of the Acquisitions Systems Protection Program and at the same time responds to several challenging questions.

Q: Dr. Elliff, What are the goals and objectives of the Acquisition Systems Protection Program (ASPP)? In other words, what are we actually trying to accomplish with this new program?

A: The goal of the ASPP is to frustrate foreign intelligence collection efforts and prevent unauthorized disclosures of the following types of valuable information.

> Weapon system technology
> Support equipment technology
> Basic research data
> Fabrication and manufacturing technology

In the past, as many as 75% of our weapons programs had countermeasures initiated against them within three years of full-scale development. We can't afford to build and field systems which are compromised soon after they are deployed. Our weapons must retain their combat advantage as long as possible.

Q: Is this program different than the present system of regulations to protect information during acquisition of new weapons? What does this give us that we don't already have?

A: It will give us much better coordination. Although DoD and the Services have had numerous regulations designed to protect information and systems from compromise, several problems have existed. The most important problem has been the lack of central direction and integration of effort. Before the Acquisition Systems Protection Program concept, some directives provided conflicting guidance to the program offices. The result was a disjointed protection attempt and an uneven security system with serious gaps and a lack of focus.

And there were a number of problems encountered in security program implementation. Security rarely received priority consideration in acquisition program development. Protection safeguards were rarely integrated into the original design of weapons programs.

Q: What is meant by integrating a "protection safeguard" into something like a weapon that is being developed?

A: An example of integrating security features into the design might be the use of embedded software. The designer can hinder the compromise of the system should it fall into the hands of a potential enemy. A software engineer could design several features into the program which would cause remote destruction if the system were lost or captured, or, could design a feature which would change or cloak the system's true ability if somebody tampered with the weapon. This is called system security engineering.

Q: How do the designers know what security features to include or integrate?

A: They must be selected to counter a known intelligence threat. Perhaps one of the most dangerous problems, before the Acquisition Systems Protection Program, was a failure to validate the intelligence threat against the system. Although an in-depth analysis was always conducted against the anticipated battlefield threat, similar attention was rarely directed against the collection threat during the development and manufacturing phases. When this analysis *was* done, it was rarely updated. As a result, most program offices did not know which countries were targeting their systems for intelligence purposes or how.

This aspect is especially important as it indicates the relative ability of the threat country to target and gain the intelligence which it seeks. From the Program Manager's perspective, the level of the threat will play a critical role in determining the level of protection required.

Q: Isn't this concept similar to the policies for Special Access Programs?

A: In a sense, yes. But under the Special Access Program (SAP) concept, the very existence of the program may be classified. As a result, really extraordinary procedures are used to maintain the security of the system. The Department of Defense establishes SAPs based upon the criticality of the program, the perceived hostile intelligence theat, or other relevant, defined threats. Obviously, this level of protection is extremely expensive. However, the key to SAP security is the degree of protection, integration, and oversight offered to these programs. The level of security applied to SAPs is exceedingly high, very selective, and involves officials at the highest levels of government.

On the other hand, the Acquisition Systems Protection concept is much broader and is directed at the normal world of weapons development. Unlike SAP systems, normal programs are developed in the public domain. As a result, these programs are much easier targets for intelligence agencies. The ASP concept focuses protection efforts on only the most critical information in these development programs, and we believe this effort will provide a cost-effective alternative to SAPs.

Q: Why do you believe this program will reduce the costs of protection?

A: The most common first impression of this program is that it will lead to additional costs and delays in the acquisition process. Both of these assumptions are false! If the ASP concept is integrated into the program, the costs should decrease and the time should be shorter. Obviously, if a program has to retrofit security features into its system, the costs and time delays will be greater.

Q: Assuming that security features are designed to protect specific technology or information, how do we determine what information or technology really needs to be protected?

A: Obviously, we do not want the program office to protect everything associated with their system. Under the Acquisition Systems Protection concept, we will protect only the most critical information elements of the weapon program. These elements are known as the Essential Program Information, Technology, or Sub-systems (EPITS). The EPITS of a system are its "crown jewels" and they must be protected at all costs.

Q: How would a program manager identify these EPITS?

A: We have devised four simple questions the manager should ask about a given piece of information:

If a foreign intelligence service obtained this information:

> could it determine how to *kill* my system?

> could it determine how to *neutralize* my system?

> could it determine how to *clone* my system?

> would I still *build it* in the present configuration?

This is the acid test. If the compromise of a particular element of information were to cause the combat system to be killed, neutralized, cloned, or redesigned, it qualifies as an EPITS.

Q: Wouldn't the EPITS be classified information in the first place and therefore subject to protection?

A: Not necessarily, especially during the research and development phase of a weapon system. As a matter of fact, our goal is to *reduce* the quantity of information which is classified, and control its declassification and release over time.

The primary vehicle we have to achieve this goal is the Time-Phased Classification Guide (TPCG). The TPCG forces the program office to look at their classified material and determine at which point within the acquisition cycle it should be downgraded or declassified.

* OPSEC is defined as the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling and protecting indicators associated with planning and conducting military operations and other activities.

Q: Having once identified a piece of information as EPITS, what does the program manager do next?

A: Once the EPITS of the system are identified, we must rely on our counterintelligence services to conduct an assessment of the relevant intelligence collection threats to the system. The objective of this process is to identify any collection vulnerabilities of the system.

In addition, our CI people will attempt to determine if any of the EPITS have been compromised earlier. The military intelligence community will also be tasked to report whether the system is already under development by other nations or if the system is unique. If our item is not vulnerable to a specific threat, there is no reason to design a countermeasure to protect it. By reducing the possible liabilities of our system, we are able to concentrate our resources against the most likely threats to our system and reduce our overall costs.

However, even if the cost of the system were to increase, the alternative to ignoring the intelligence theat to unique U.S. weapon capabilities is even worse. If we lose our technology, we will lose our ability to maintain the battlefield edge we had in Desert Storm and fuel the proliferation of sophisticated weapon systems to potential adversaries. As a result, we will place our soldiers at risk. We are particularly concerned about regional military powers to which technology may be transferred by our friends and adversaries alike.

Q: ASPP is beginning to sound a lot like operations security. Is it essentially the same thing but in a different context?

A: OPSEC deals with observable activity and is in fact an integral *component* of the ASPP system. The Program Protection Plan should specify whether and at what stages an OPSEC plan is needed. However, OPSEC, by itself, is not the total ASPP package.

Q: What about the traditional security disciplines such as information systems security, physical security, or personnel security? How do they figure into this program?

A: As with OPSEC, these disciplines are not complete packages by themselves. Rather they are integral components of the complete protection package. Each Program Protection Plan for a specific weapons system should normally affirm the need to apply established regulations in each of these disciplines. In some cases, gaps may be identified which are not covered by one of the traditional security disciplines, especially in the testing phase.

Q: Will the ASPP concept be extended by the DOD to government contractors?

A: Program protection is the coordinated implementation of existing policies, including industrial security, which are integrated into a plan for an individual weapon system in acquisition. There will be minimum impact on the industrial community because each plan will affirm the need to follow the Industrial Security Manual. And by the way, no legal problems are envisioned.

Q: Speaking of Industry, How will the ASPP concept be integrated into the new National Industrial Security Program (NISP)?

A: Presently, the NISP is still evolving. The NISP is designed to develop common security standards, enhance security, and reduce the costs of protection. In many ways, the ASP concept is similar in its goals. Acquisition Systems Protection is a management tool to ensure that requirements levied on the industrial community are appropriate. For example, managers will focus at early stages on the need to classify information and to include security safeguards in the engineering design.

Q: Considering the demise of the Soviet state, why are we implementing this program now?

A: Although the Soviet Union has dissolved, a massive intelligence collection capability still exists and responds to Russian state interests. In particular, Russian military intelligence (GRU) continues vigorous clandestine collection against U.S. military targets. The greatest risk may be to fuel Russian sales of weapon systems to regional powers, against whom U.S. forces may be deployed in future conflicts. The sale of the Kilo-Class submarine to Iran underlines this new level of competition.

However, the threat to acquisition systems is not limited to the former states of the East Block. As tensions have decreased, many countries have transferred intelligence activities to economic and industrial espionage. In a world of growing economic competition, the threat from these non-traditional adversaries is a significant danger to U.S. programs. Both friends and adversaries seek U.S. technological secrets so they can copy and counter the capabilities and exploit the limitations of U.S. weapons.

Q: Obviously, we have a lot to learn about the current threat and how the program will work. Who will provide the training to those people who will be responsible for protection planning?

A: For now it rests with the Acquisition Systems Protection Office (ASPO). Presently, the officers assigned to the ASPO travel all over the country to help program offices with their protection programs. In addition, they receive numerous calls each day on the protection process.

In the long term, the responsibility for training will transfer to the DOD Security Institute (DODSI) and the Defense Systems Management College (DSMC). DSMC will have the primary responsibility for training the acquisition personnel on protection planning. DODSI will have the primary responsibility for training the security personnel on protection planning.

Q: Dr. Elliff, we have covered a lot of territory, but is there anything you would like to add?

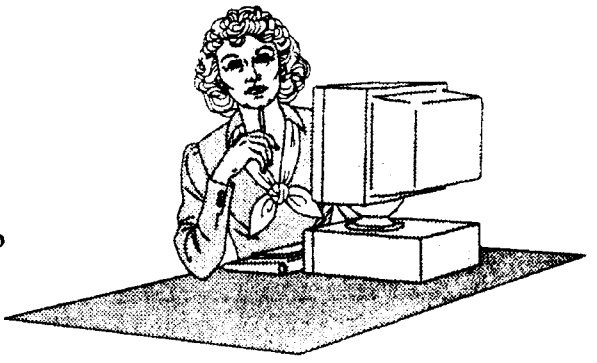
A: Yes, a last bit of advice. The ASP concept is a new program. As such, we are still in a transition phase. The concept is gradually winning acceptance throughout the acquisition, security, and intelligence communities. Considering the continued seriousness and changing nature of the threat to U.S. technology, we must inform as many people as possible about the need for an approach that integrates security measures across disciplines. Program Executive Officers and Programs Managers need to realize that this requirement exists and that the goal is to focus security countermeasures where they will do the most good. We believe this approach will be cost effective for the acquisition community.

Video . . .

Is Your PC Data Safe?

Date: 1992 Length: 21 min. Cost: $325.00
15-day preview fee: $27.50 (includes shipping/handling)

Order from: Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178



Summary: This computer security training program for government contractors comes with a 21-minute video, instructor's manual, and student guide materials. Video shows the importance of following the guidelines in Section 8 of the Industrial Security Manual, and your SPP. Dramatization tells the story of a new company president with a poor security posture and the tips he receives from his ghostly colleague. Video is closed captioned for hearing impaired. Produced by Pro Star International. Program also comes in a second version: Protecting trade secrets and proprietary information.

announcing . . .

AIS Security Procedures For Industry Course (AIS-I)

The 3½ day AIS-I provides contractors with practical experience in reviewing AIS Standard Practice Procedures (AIS SPPs) and conducting AIS Self-Inspections. The Defense Industrial Security Program requirements for processing classified information in data processing and office automation systems are explained, together with supporting rationale.

Topical areas include: discussion of AIS security procedures and guidelines; and applicable AIS SPP outlines prepared and distributed by DIS activities. Using guidance provided during the course, students will review an AIS SPP for a microcomputer system and inspect the system in accordance with Chapter 8 requirements of the Industrial Security Manual (ISM).

The course will be held in residence on the following dates:

April 20-23, 1993 August 2-5, 1993

September 21-24, 1993 (held in Washington, DC)

There is no tuition for the course and a security clearance is not required. To be eligible for attendance, students must prepare or have oversight responsibility of AIS Approval and AIS SPPs. Upon acceptance to the course, students must complete a series of Work-Ahead-Modules (WAMs) which will be issued to them approximately one month prior to the commencement of the course. Class size is limited, so registration is accomplished on a first come, first served basis.

For course details, call the AIS Division, (804) 279-5309 or 279-4187.

Mail this page to: Attn: Registrar
DoD Security Institute,
c/o DGSC
Richmond, VA 23297-5091

Your Name Mr./Mrs./Ms._____

Position _____

SSN _____

Company Name _____

Address _____

_____

_____

Telephone _____

Supervisor _____

Course Title AIS Security Procedures for Industry

Course Dates _____

reprinted from the May-June 1992 issue of Program Manager, a journal of the Defense Systems Management College

Acquisition Systems Protection

Keeps Sharp DoD's Competitive Edge

by Edward P. Casey

A new term has entered the lexicon of program managers and others involved in DoD acquisition. With the February 1991 publication of DoD Instruction 5000.1, "Defense Acquisition Management Policies and Procedures," acquisition system protection (ASP) has been mandated as the means by which defense systems and technical data in the acquisitions cycle will be protected from foreign intelligence collection and unauthorized disclosure. New policies on program protection and technology control have been established to safeguard U.S. technological superiority, economic competitiveness and the uncompromised combat effectiveness of U.S. weapons systems.

"Acquisition Systems Protection is not traditional security," in the words of Colonel Dave Evans, former Chief of the Acquisition Systems Protection Office (ASPO), which has been established as a part of the office of the Director of Defense Research and Engineering (DDR&E), Under Secretary of Defense (Acquisitions) (USD(A)).* Colonel Evans said:

ASP encompasses and makes use of traditional counter-intelligence and security disciplines, but it is an acquisition function. The program manager is responsible for the protection of the information and technologies entrusted to him. The protection of the system from compromise is every bit as essential to its mission success as its ability to perform up to specification or the fact that the system was delivered on time and within cost.

As demonstrated most dramatically in the Persian Gulf War, the technical superiority of U.S. weapons systems has played, and will continue to play, a significant role in guaranteeing that U.S. forces will prevail in any military conflict. Gaining and maintaining the technological edge has given the United States a wider range of strategic and tactical options and allows U.S. forces to achieve military objectives at far less cost in material and, more importantly, in human lives.

While the performance of U.S. weapons in the Gulf War was highly impressive, their success was due in no small measure to the absence of effective countermeasures in the hands of our Iraq adversary. Of critical concern to U.S. strategists in the 1980s was the fact that the technological lead times in which U.S. weapons were judged effective against a potential adversary were, in fact, consistently shrinking. As a result, systems which were developed and fielded with an anticipated effective life span of 15-20 years were, in many instances, rendered militarily ineffective in 2-3 years by the fielding of adversary countermeasures. In such instances, years of effort and billions of dollars in research and development costs were negated by successful adversary technological development. Where possible, the U.S. response involved costly and time-consuming modifications and upgrades to its weapons systems. In many cases, the original levels of superiority and military effectiveness enjoyed by the U.S. system could not be fully restored. The technological edge, upon which so much of U.S. defense strategy depended, was effectively being drained away.

As the costs and dangers of this technology drain became more and more apparent, both the

* *In September 1992 responsibility for the Acquisitions Protection Office was moved to ODASD(CI&SCM). Mr. Doug Cavileer is presently acting director for ASPO. He can be reached at (703) 697-2242.*

Congress and the Department of Defense called for studies into the roots causes, and potential solutions, for a problem which was seen as posing a serious threat to U.S. national defense. The 1980s has been referred to in the U.S. press as the "decade of the spy." During the decade, more than 40 American citizens were apprehended by U.S. counterintelligence agencies acting as agents for foreign intelligence services; however, espionage was by no means the only threat to grow during the 1980s. Considerable advances were made in the technologies used to collect and analyze imagery and signals intelligence. The number of U.S. allies and potential adversaries possessing these sophisticated techniques increased considerably during the decade. Analysis of the intelligence threat environment facing the United States in the late 1980s identified two disturbing trends: one, foreign intelligence targeting of the U.S. military and civilian defense industry was increasingly directed at RDT&E and "high technology" programs; two, serious vulnerabilities in the protection of these programs were facilitating the technology drain.

In early 1990, a special panel was convened at the direction of the Under Secretary of Defense (Acquisition). The Protection of the U.S. Technical Lead (PTL) Review Group was formed to examine the issues of threat and the need to protect U.S. technology in systems acquisition. The PTL Review Group's report made a number of findings and recommendations. Key findings included:

1) System classification guides were the only program documents dealing with protective measures. They, however, were merely item-by-item classification lists and did not set forth comprehensive goals and objectives for program protection.

2) There was no institutionalized process to determine what measures a program should employ to protect critical information.

3) Security and protective measures receive a low priority for the resources and manpower available to program managers.

4) Security and protective measures at test-and-evaluation sites have a low priority compared to other infra-structure improvements.

5) There was no program protection training for program managers and other acquisition personnel.

Key recommendations of the PTL report included

1) At the program-management level, a system protection plan should be required for major acquisitions to address the issue of protecting critical information.

2) At the program-management level, counterintelligence/operations security surveys should be performed for every major system.

3) At the DoD level, a system should be established to track funding requirements for protection measures.

4) At the DoD level, system-protection training guidance should be developed.

5) At the DoD level, a new USD(A) element should be created to develop a protection master plan and review system protection plans.

At the same time as the PTL Review Group was working within the DoD, the congressional review process for the FY91 DoD budget further acknowledged the need for greater protection of technologies in the acquisition cycle. The House Armed Services Committee, the House Appropriations Committee and the Senate Select Committee on Intelligence all addressed the acquisition systems protection issue in their reports.

Perhaps most comprehensive was the language contained in the House Armed Services Committee report. Under the heading of "Security Improvement Program," the report, "directs that the DoD begin to correct security deficiencies during FY91 and that it complete the process within five years ... During FY 91, the Office of the Secretary of Defense shall conduct comprehensive security surveys of test facilities, laboratories, and other RDT&E facilities and shall ... devise an overall strategy identifying and prioritizing recommended security improvements ... The existence of a dedicated component within the Office of the Secretary of Defense, with sufficient authority and high-level attention, appears critical to successful and timely completion of the program. Due to past difficulty in identifying funds requested for, and actually spent on, counterintelligence, countermeasures and security programs, all DoD RDT&E facilities henceforth shall group and identify such allocations within relevant budget documents."

The congressional reports specifically mandated three things.

1) Establishment of an office for acquisition systems protection oversight within the Office of the Secretary of Defense.

2) Development of an overall protection strategy that identifies and prioritizes recommendations for correcting acquisition-related security deficiencies.

3) Specific identification of acquisition systems protection funding.

In 1990 and 1991, the Department of Defense moved quickly to implement congressional instruction and recommendations of its PTL Review Group report.

In August 1990, the three military departments signed a memorandum of agreement establishing the Joint-Service Acquisition Systems Protection Program (JASPP). The JASPP is responsible for development of standardized capabilities for acquisition systems protection, review of procedures and recommendations of improvements, sharing lessons-learned in protection surveys, and for planning joint investments in studies, training and related efforts. In January 1991, USD(A) formally established the ASPO within the office of the DDR&E, Deputy Director for Plans and Resources (P&R). The ASPO was assigned a number of functions. Chief among them were development of a DoD ASP Master Plan, review of security classification guidance and program protective measures for each of the major acquisition programs, and providing an assessment of program protective measures for each major acquisition program to the appropriate Defense Acquisition Board (DAB) committee before each milestone review. By the latter part of 1991, the ASPO had begun this program-protection review process. In some instances, program protection plans were found to be incomplete.

With the JASPP and the ASPO in place and a DoD ASP Master Plan being created, a means was needed to promulgate and enact the new ASP policies throughout the entire acquisition community. That means was found in the publication of DoD Instruction 5000.2, and particularly in Part 5, Section F, of the new instruction, which is devoted to program Protection and Technology Control. This section specifically requires that "a comprehensive protection and technology control program shall be established for each defense acquisition program to identify and protect classified and other sensitive information."

As further defined in Part 5, Section F, protection and technology control involves the application of all traditional security disciplines and counterintelligence into a coherent protection program, and integration of this comprehensive protection effort into the acquisition process. At the core of this effort is to be a Program Protection Plan (PPP). A tailored plan is to be created for each defense acquisition program. The plan and protection efforts are to "encompass program related activities at test centers, ranges, laboratories, contractor facilities, and deployment locations as required to provide protective measures for all aspects of the acquisition program."

According to Colonel Evans, "The specific function served by the PPP is twofold: first; it promotes the early identification of all the essential program information, technology and system, or 'EPITS', to be protected; and second, it creates a comprehensive protection management plan outlining the measures to be taken to protect the weapon system throughout its life cycle."

The PPP is to be developed before Milestone I and will be updated for subsequent Milestones. The plan is to specifically contain a description of the system or program and its elements requiring protection, the EPITS. The plan must define existing or anticipated intelligence collection and security threats and the identified program vulnerabilities, which place the EPITS at risk, as the program moves through the acquisition cycle. Countermeasures designed for each environment in which the program or system will exist must be described. Protection costs (personnel, equipment and funding) required in each acquisition phase are to be identified. The PPP is to contain annexes describing these requirements in each acquisition phase, along with attachments, like a Security Classification Guide and a Technology Assessment/Control Plan and Delegation of Disclosure Authority Letter for planning and controlling any transfer of program information or technology to foreign governments.

The implementation of acquisition systems protection and program protection planning throughout the acquisition community is a considerable undertaking. From a program manager perspective, three basic questions may come to mind. Why do I need ASP? What is the difference between ASP and security measures that previously have applied to my program? How am I supposed to implement ASP in my program?


STEALTH

In light of U.S. victory in the Cold War, the likelihood of nuclear conflict and of major armed conflict in Europe involving the United States seems to have diminished significantly. From an intelligence perspective, however, the threat to U.S. interests actually may be increasing. While we no longer face the collections efforts of "hostile intelligence services," a term the United States applied to the intelligence apparatus of the former Soviet Union and its former Warsaw Pact allies, we face the threat from a growing number of "foreign intelligence services," a term the U.S. intelligence community uses to recognize that, in the post-Cold War world, governments of former enemies and allies will use their intelligence assets to pursue what they perceive as their legitimate national interests. Intelligence collection, particularly as it supports technological advancement and advantage in economic competition, is a tool likely to be used by all possessing it. In fact, the end of the Cold War freed considerable intelligence collection assets that were devoted to targeting military order-of-battle information to be redirected against defense-related RDT&E and acquisition system targets.

Development of acquisition systems protection has proved to be fortuitous in the face of an increasingly complex and sophisticated post-Cold War intelligence theat. The United States faces an era of increased multinational cooperation in matters of defense and increased international competition in economic affairs. This seeming dichotomy opened significant new collection venues to foreign intelligence services through areas like joint research and development, dual-use technologies, foreign ownership of, or interests in, U.S. companies, and U.S. foreign military sales, at precisely a time when their interest in, and need for, such information is increasing. Targeting U.S. critical technologies is not motivated solely by military concerns. Competitor intelligence and economic and industrial espionage by nations and organizations seeking competitive advantage is on the rise and is likely to pose a significant threat in the post-Cold War world.

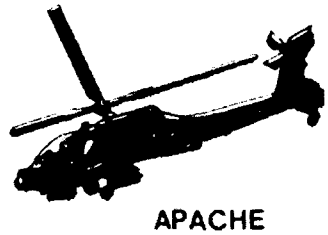
"As we saw in the 1980s, our traditional security methods were simply inadequate for the protection of critical technical information," Colonel Evans said. He further stated that "We could protect our classified information, but still lose the essence of a program through gaps in our protection coverage. ASP is intended to close those gaps and to take into account the protection of information which may not be classified but which is nonetheless critical to the military effectiveness of the system."

Whereas traditional security methods establish a baseline of security standards in each separate discipline and then attempt to bring program activities into compliance with those standards, ASP takes a more holistic and synergistic approach. Starting with a detailed analysis of the program or system in all of its phases and locations, ASP seeks to identify the "crown jewels" of the program, the EPITS which a potential adversary or competitor must obtain to neutralize or copy the system under development. The ASP recognizes that the intelligence collection process is a mosaic in which a larger, classified picture can be assembled from smaller, sometimes unclassified, bits. Consequently, ASP defines the EPITS to be protected as not only classified material, but as unclassified sensitive data, if its loss will provide critical insights into compromise of the system's military effectiveness.

Rather than establishing its protection standards from a generic security baseline, ASP makes extensive use of counterintelligence threat analysis, which looks at the actual and anticipated foreign intelligence collections threats facing the program in each of its environments. Acquisition systems protection takes into account not only the developmental and manufacturing environment of program management centers and contractor facilities, but environment of the laboratories and ranges where the system will be tested. The threat and resultant vulnerabilities in each environment are

surveyed and analyzed to ensure that a program is afforded what is termed "horizontal protection."

"Horizontal protection," according to Colonel Evans, "is a concept of ASP which recognizes the need to provide full and equal levels of protection to the EPITS in every environment in which they reside. It does no good to protect an item at one time and location, only to give it away at another. Horizontal protection is meant to ensure that once a technology is deemed critical, it is adequately protected not only in all parts of an individual development program, but throughout the U.S. acquisition and RDT&E community as well. This is especially true where a critical technology may be common to separate weapons systems being developed independently by different Services. One role of the ASPO is to develop the means to identify and coordinate such instances throughout the DoD."



APACHE

Identifying the EPITS and analyzing threats and vulnerabilities are the first two steps of the protection process. Next, ASP requires that detailed, tailored protective measures be designed and applied to *neutralize the foreign intelligence* threat. It is in the application of these protective measures that ASP make use of the traditional security disciplines, such as physical security, personnel security, information security and communications security. The ASP is not a new security discipline; rather, it makes use of existing disciplines and enhances their effectiveness by tailoring their application to specific requirements of the environment in which the program resides. "For example," cited Colonel Evans, "in the contractor world, Industrial Security needs to work as the base. Over and above that, Program Managers have to consider the specifics of threat and vulnerability and must place in their contracts those protective measures which are needed beyond that base."

The creation of a PPP for each acquisition program as called for in DoD Instruction 5000.2 is not intended to replace the existing security infrastructure. Rather, it is intended to maximize effectiveness of security by fully integrating it into the acquisition process. By establishing program protection as a direct acquisition responsibility (and a program manager's responsibility), the required management emphasis for a successful protection effort will be assured and meaningful protection provided to truly critical information and systems.

Implementation of ASP and creation of a PPP present the program manager with significant improvements over previous methods that failed to integrate protective measures into the acquisition process in a timely and comprehensive manner. Unlike the past, where costly system modifications and security retrofits had to be added to a program in an attempt to make up for previous technology losses, ASP is not intended to be an "add-on." Rather, it is a cost of doing business up front and is intended to be factored in from the early stages of system development.

According to Paul Blatch, RDT&E Program Protection Coordinator for the Chief of Naval Operations, Chairman of the JASPP and a leading figure in the development of the ASP concept:

> Program Managers have to concurrently understand the technologies residing in their program, the supporting security resources at hand and the process involved in identifying EPITS. This understanding, along with the ability to analyze threat and vulnerabilities, is the key to the design and application of countermeasures that will insure the adequate protection of their program. Program Managers need a focal point for ASP within their program staff that can involve program technical experts in the identification of EPITS and can facilitate the support of security and counterintelligence personnel in their operation. They need to involve their budget and contracting staff in determining realistic cost estimates and in seeing that ASP requirements are written into contract documentation. When they take their program into a lab or onto the test range, they need to insure that their protection requirements will be adequately met by the existing facility security and if not, that necessary upgrades are put into place by the time they are needed. Program Managers need to arrange for ASP training for personnel on their staff whose involvement will be crucial in the ASP process. Properly trained and supported, Program Managers and their staffs will be able to design Program Protection into their

programs which is comprehensive, integrated, affordable and executable, and which will absolutely enhance mission success.

Acquisition systems protection is a complex undertaking, but one which seems particularly appropriate and meaningful as the U.S. defense establishment begins to adjust to the realities of the post-Cold War world. As the Department of Defense moves to a new acquisition strategy that emphasizes research over production and seeks to maintain technological advances despite greatly reduced procurements, the need for enhanced protection of prototype systems for prolonged periods will become absolutely critical to the system's military effectiveness when it is eventually fielded. In the Statement of National Military Strategy prepared by General Colin Powell, Chairman, Joint Chiefs of Staff, in January 1992, the role of ASP in the evolving defense situation was described as follows:

> Beyond the requirement for a reconstitution capability is the compelling need for continued and significant R&D in a wide spectrum of technologies, applications and systems.
>
> ...We need to protect the capability to produce the world's most technologically advanced weapons systems, but only if required.
>
> ...The United States must continue to rely heavily on technological superiority to offset quantitative advantages, to minimize risk to U.S. forces, and to enhance the potential for swift, decisive termination of conflict. We must continue to maintain our qualitative edge. Therefore, advancement in and protection of technology is a national security obligation.

Mr. Casey, a program protection specialist with Beta Analytics, Inc., served for 20 years as a special agent and counterintelligence officer with the United States Air Force Office of Special Investigations. Mr. Casey plans, integrates, and implements systems protection programs and teaches acquisition systems protection and related topics.

Video . . .

Friend and/or Foe, The New Espionage Challenge

Date: 1991 Length: 20 min. Medium:VC

Order from: Pro Star International Cost: $21.00 includes shipping
P.O. Box 21526
Salt Lake City, UT
1-800-775-0761
fax: (801) 943-5178

or FilmComm Cost: $26.00 includes shipping
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

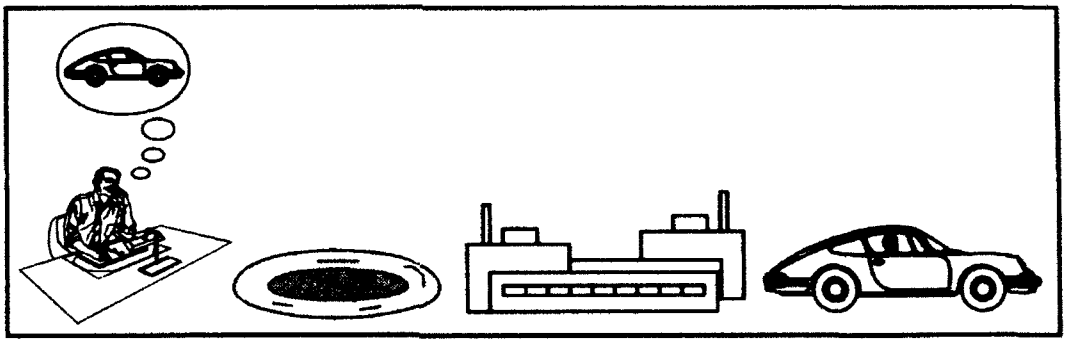
Summary: An up-to-date film on the changing threat to national security showing that our international friends are sometimes our foes. When any country's need or desire for our technology spurs them to illegally acquire non-exportable U.S. technology, it has passed from friend to adversary. And attempts are being made all the time. The cooperation among U.S. Customs, American industry, and the FBI is helping to curb the increasing flow of illegal export. This 20-minute film clearly states the enormity of the problem and what you can do to help prevent further loss of our nation's top security priority: its competitive edge in world technology. Produced by Hughes Corporation in cooperation with the FBI and U.S. Customs. Closed captioned for the hearing impaired.

Acquisition Protection For The Layperson

by Cynthia Kloss

Much has been written on acquisition security during the past year. Also known as acquisition systems protection, the initiative to formalize the protection of developmental weapons systems was implemented in the February 1991 revision of the DoD Directive 5000.1, Defense Acquisition. The requirement is to apply protective measures throughout the acquisition lifecycle.

Example: We need to produce a new model car that is very energy efficient and that will beat Toyota, GM, Ford, etc. in the economic marketplace. The design of the car will include new and advanced technologies (for a light weight product with remarkably improved gas mileage).



Sounds fine, but what exactly is an acquisition effort, and how do I protect it?

An acquisition program is a directed, funded effort that is designed to provide a new or improved materiel capability in response to a validated need. It is protected through the judicious use of countermeasures appropriate for the program.

When a component of the Defense Department identifies a deficiency in its combat effectiveness, a series of events and decisions occur involving hundreds of individuals in dozens of staff sections ultimately culminating in the development of a weapon system. The system may be easier to understand if we place it in a context that we are familiar with.

The acquisition lifecycle consists of a series of developmental activities known as phases. Starting with a mission need, the phases of activities are concept exploration and definition, demonstration and validation, engineering and manufacturing development, production and deployment, and operations and support. Using an example based on a commercial need, we will examine activities occurring in each phase and the related protection concerns.

Determination of Mission Need: (Simply stated, what is the requirement or need?)

The analysis of mission need determination would consist of exploring options already available and early identification of essential features of the car. In our example, the need is to build a more energy efficient car. For protection planning, what would the key mission features of the car be? What are the essential program information, technologies, and systems (known as EPITS) that if compromised would negate any competitive edge we may gain with the new automobile?

In our example, the key technologies involved have to do with:

a. the materials used in the car (low weight, high strength body/frame combination); and

b. the high efficiency engine (revolutionary combustion composite that is used in each cylinder).

Looking at the projected collection threat, does the competition own the same technology or are they actively pursuing the same? If known, would a competitor (adversary) be able to replicate the technologies? Can these technologies be protected against the known collection threat during the design, development, testing, and initial production phases? Our goal is to reach the market before our

competitors with sufficient lead time to corner the automobile market.

Concept Exploration & Definition (What are the options?): During this phase, we examine the available options to meet the need, focusing on the two general areas of technologies. We also explore alternative technologies that have potential for satisfying the basic need. Which materials will do the job, and is there a potential for mass production?

While exploring potential options, we again look at the collection threat and determine what protection is required to achieve the program goal of manufacturing this car. The threat may be more extensive at certain points in the developmental process. We then must examine the threat in relationship to the operating environment to pick out the points where the program is vulnerable and the technologies can be exploited. We also must address the cost associated with the protection.

Example: The alternative technologies have been evaluated and we now start to plan our protection program. The most essential information elements of the program are identified, the collection threat defined and vulnerabilities addressed. The document which contains this analysis is the Program Protection Plan (PPP).

Demonstration and Validation (Do the options chosen work?): In this phase we begin to design the product and build working models or prototypes. We may subcontract for individual components of the car, such as the engine and try different design approaches. The prototypes will be tested and evaluated at the laboratory or in the factory.

How should we protect the technologies during development of the test models? And when testing is complete, how will we protect the test reports, drawings, technical specifications, etc.? Will the protection implemented at the factory be the same as at the proving grounds?

Example: In implementing the PPP, we must monitor the effectiveness of protection for the EPITS. Countermeasures are implemented for the vulnerable areas. The test engines will only be run in secure areas. Only selected engineers will be allowed to handle the combustion composites and their technical documentation. Documentation and samples of the body materials will be guarded at all times. We monitor the prototypes for new, unpredictable vulnerabilities that may arise. The approved PPP will be reviewed, revised, and updated to ensure protection during the next phase of development.

Engineering & Manufacturing Development (selecting and refining the design for production): This is where the design and technologies are selected and matured for entering production. Manufacturing and production processes are determined and validated, and enough cars are built to prove the design. Initial units are tested under realistic road conditions to make sure they can deliver the performance stated in the original need statement.

Example: The protection we previously implemented focused on the existence of our effort to apply unique technologies for an energy efficient car. Since the number of people needed to build the preproduction models increased, and publicity is necessary to generate sales, we can say that the collection threat has changed. Industry magazines are a potential threat since they will likely try to gain access to details about the car. Another protection issue is that the preproduction cars must be transported to additional testing and manufacturing facilities and we will have to bring in selected dealers to promote eventual sales. All of these activities must be factored into our total program protection plan which is modified prior to going into the next phase.

Production and Deployment (build and transport to dealers): Initial production on the new model cars will be started and finished products will be transported to dealers for introduction into the market place. Once we introduce the cars, the essential information no longer requires protection however the sustainment may create new EPITS.

Example: The car is now in production and the supporting logistics are in place to ensure that the car can be sustained. What happens if problems occur with the car and modifications are needed? Perhaps we are already looking at improvements over the technologies for next year's model. If additional protection is needed, we must communicate to the consumer and those providing support for the car the additional protection needs.

This concludes the discussion of a commercial acquisition effort which is similar to that involved with weapon systems acquisition. The phases and

decision points all have parallels. Now we will apply the same process when developing a new weapon system.

Determination of mission need is done by the user community (the same agency that will eventually receive the new weapon system). A military component identifies a new and emerging threat (*e.g.*, a new radar intercept system with a unique acoustic signature). After evaluating existing tactics, doctrine, training, and current systems, the component determines that a new, smart missile system with acoustic sensor is required. Thus a need is established.

Concept exploration occurs when a series of possible solutions are identified and examined by government, industry, or both. The goal is to mitigate the new and emerging threat; the way this is done will vary considerably. Studies of possible solutions are contracted for and evaluated. The most promising solution advances into the next phase of the lifecycle.

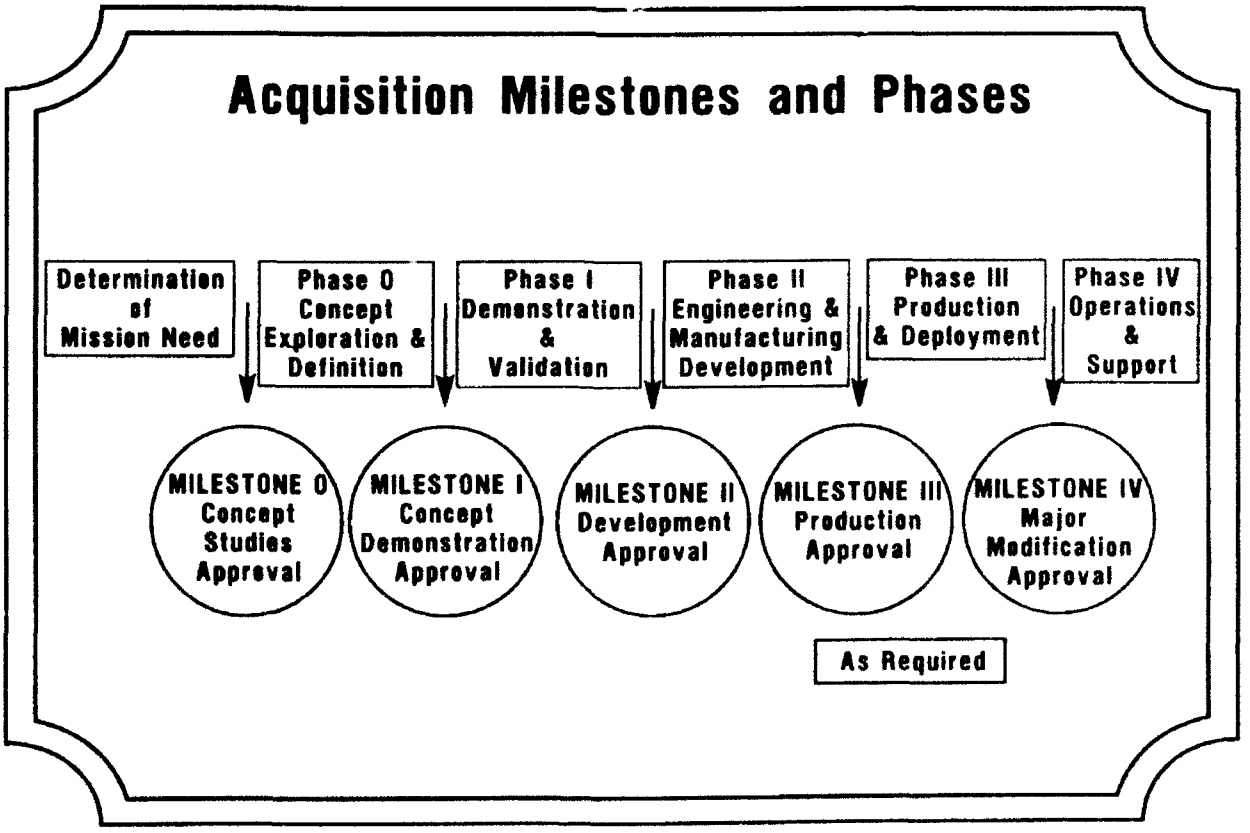
Demonstration and validation of the promising missile system designs are done using prototypes. Once the technology is proven, a decision to continue the developmental effort for the new missile system is made.

Engineering and manufacturing development of the selected missile option further defines the final design of the weapon. Once the final design is established, proven, and supportable, the weapon system is available for initial production runs.

Production and deployment of the missile system is determined by the overall need of the user. Questions regarding which units will receive the new missile systems, how many total missiles are required, what delivery schedule is needed, how will the missiles be fielded, who will train the receiving units, etc. are answered.

Once fielded, the missile systems are monitored for continued viability in relationship to the threat and overall war-fighting capabilities.

Do you see the parallel between the new car and the missile system? Application of protection throughout the acquisition lifecycle will ensure that both the car and weapon system are fielded while maintaining a technological advantage that has not been prematurely exploited.



Training Resources for the ASPP

A series of exportable training modules have been developed to provide additional information on acquisition systems protection.

- Introduction to Acquisition Systems Protection: A 90-minute course of instruction designed to orient personnel on the basics of acquisition systems management and introduce the fundamentals of the protection program.

- Acquisition Systems Protection (Advanced): A 4-hour lesson designed for practitioners developing program protection plans.

- Acquisition Systems Protection for Acquisition Professionals: A 90-minute lesson focusing on the enabling disciplines for protection planning such as security countermeasures, counterintelligence support, operations security and intelligence support.

Projected training tools include video tapes and correspondence courses.

For more information on these products contact your organization's protection specialist or security manager. Additional information is also available from the Acquisition Systems Protection Office or the Defense Security Institute, ATTN: Cynthia Kloss, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091.

LEXICON

Acquisition Program -
Directed, funded efforts designed to provide new or improved materiel capability in response to a validated need.

Acquisition Systems Protection (ASP) -
The safeguarding of defense systems anywhere in the acquisition process. The activity integrates all security disciplines, counterintelligence, and other defense methods to deny foreign collection efforts and prevent unauthorized disclosure which could compromise combat effectiveness.

Defense Acquisition Board -
The senior general management review board chaired by the USD(A). This is the primary forum used by DoD to provide advice, assistance, and recommendation on all aspects of the DoD Acquisition System.

Essential Program Information, Technology, or System (EPITS) -
That information about the program, technology and system that if compromised would degrade combat effectiveness or shorten the combat effective life of the system.

Program Protection Plan (PPP) -
A comprehensive protection and technology control program established for each defense acquisition program to identify and protect classified and other sensitive information for hostile intelligence collection or unauthorized disclosure.

Just released . . .

a new, 18-minute video based on interviews of convicted espionage felons, designed to motivate employees and military personnel to support personnel security programs through timely intervention.

You Can Make a Difference

First in a series of six videos — each of which will focus on a different aspect of espionage, and what can be learned, from the point of view of the offender.

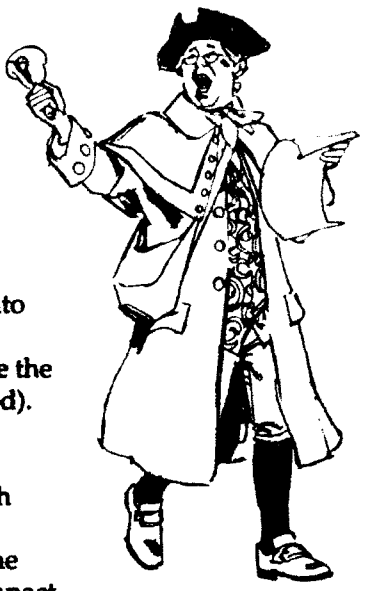
You Can Make a Difference is marked For Official Use Only. It is not releasable for public viewing or to the media. Now being distributed to Federal agencies and departments, cleared contractors may obtain a copy by written request through FilmComm Inc. *Prepaid* cost is $21.50 plus $2.50 for shipping for 1/2". *Invoiced* requests are $23.50 and $2.50 for shipping. (For 3/4" add $10.00.) For additional details, please call FilmComm.

For government contractors: Because this is an FOUO product, we ask you to certify in your order that, when received, "this video product will be used only for the training and education of employees or personnel in support of a federal government security program."

To order:
FilmComm Inc.
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

This video has been produced by the Department of Defense Security Institute in cooperation with the National Advisory group for Security Countermeasures and Project Slammer.

The NISPOM is coming!
The NISPOM is coming!



DoDSI is offering several training options for transition into the NISP.

On January 6, 1993, President Bush signed into being the National Industrial Security Program (NISP) which will bring uniformity to the way classified information is protected by non-government organizations.

Currently, most government contractors are under the Defense Industrial Security Program (DISP). DISP policy originates in DoD, and the Defense Investigative Service inspects facilities involved in the program. But besides the DISP, there are other industrial security programs operated by other government organizations. Each program involves different policies and procedures and this translates into different requirements being levied upon the contractors from those organizations. This has been a burden on contractors.

In contrast, the NISP will bring all industrial security programs under one program. The details are being worked out and the next step will be the publication of a NISP Operating Manual (NISPOM). The NISPOM will be available by January 1994. In the coming months you will hear much more about the NISP and the changes it will produce. DoDSI is taking an active role in this process. We are in the process of putting the proposed changes into our existing course material (even before the NISPOM is published). We plan to talk with government policy makers and also with the contractor community to identify the changes and their impact.

DoDSI will offer several options for those of you seeking training to transition into the NISP.

- **The correspondence courses many of you took as an introduction to the DISP are being rewritten to reflect the NISP requirements. (Watch for more specific announcements.)**
- **The Industrial Security Management Course is being transformed into the NISP Facility Security Officer Program Management Course which will cover all aspects of the NISP.**
- **The Advanced Industrial Security Management Course is designed to address current issues in the program, and will include transition training for experienced Security professionals.**

We are assessing the viability of offering one- or two-day Transition Training Seminars covering only the major changes from the existing DISP to the NISP. If you are interested in attending a seminar, please return this questionnaire.

Name: _____ Company: _____ Phone: _____

Address: _____

- ❑ I would attend a one or two day Transition Training Seminar offered in Richmond, VA.
- ❑ I would attend a one- or two-day Transition Training Seminar if offered in the following area:
  - ❑ Southern California
  - ❑ Northern California
  - ❑ Boston area
  - ❑ New Jersey
  - ❑ Washington, DC area
  - ❑ Southeastern United States
  - ❑ Dallas, Texas area
  - ❑ Mid-West
  - ❑ Phoenix, Arizona area

Mail to: Wayne Lund, DoD Security Institute, c/o DGSC, 8000 Jefferson Davis Highway, Richmond, VA 23297-5091

National Classification Management Society
29th Annual Training Seminar

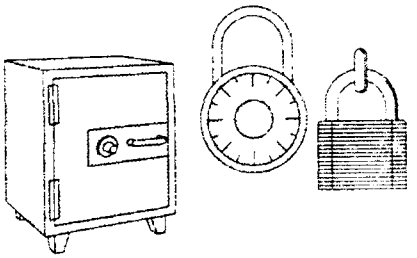
Don't Gamble With Our Country's Security

June 29 - July 1, 1993
Atlantic City, New Jersey

If you would like more information, contact
NCMS Mid-Atlantic Chapter Registration
Dean Wright (908) 919-2473
or
Executive Secretary Eugene Suto (301) 231-9191

Video . . .

Safes, Locks, and Videotapes



Date: 1991 Length: 12 min.

Order from: FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

Cost: $26.00 includes shipping

or Pro Star International
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178

Cost: $21.00 includes shipping

Summary: This video talks about the different GSA containers and locks; container labels, how to inspect a container and lock. How to change a combination. Lists security device manufacturers. Comes with pamphlet that provides additional information. Produced by the Defense Security Institute. Closed captioned for the hearing impaired.

Lethal Weapons Too

We have quantities of a computer security poster available for the asking. Originally produced by American Forces Information Service. Just call or write for your free copy. 17" x 22" color poster comes folded flat.

(804) 279-4223
Attn: EPD
DoD Security Institute
c/o DGSC
Richmond, VA 23297-5091

Video . . .

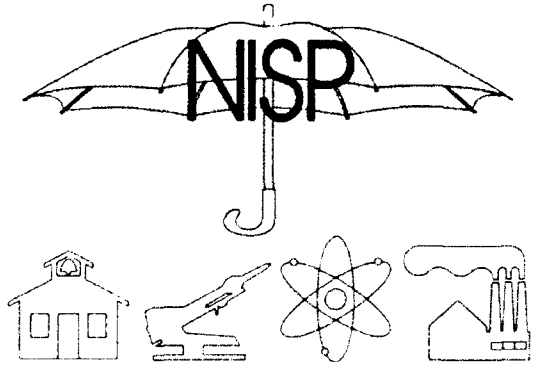
National Industrial Security Program

Video #1 NISP Status Date: March 1992 Length: 09:45

Video #2 NISP Overview Date: February 1991 Length: 17:26
NISP Status Date: March 1992

Cost per videotape: $17.50 for VHS $27.50 for 3/4"
(add $2.50 for shipping)

Order from: FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325



Summary: The Boeing Company has been involved in a national effort to replace the many redundant Government security programs levied on industry with one cohesive, integrated set of requirements. This program has become known as the National Industrial Security Program (NISP). Boeing, in support of the NISP, has produced two videos: an overview of the program and more recently an update status video.

DISSPATCH

The INFOSEC newsletter from the Defense Information Systems Agency

Keep abreast of the latest and greatest in information systems security (INFOSEC)... read articles from the forerunners in INFOSEC ... find out about upcoming conferences in a monthly newsletter!!

The Defense Information Systems Security Program (DISSP)* has been chartered to manage the implementation of INFOSEC with DoD programs and the insertion of multilevel security technology. One of our tasks is to coordinate an INFOSEC awareness program. As part of this program, DISSP has begun printing a monthly newsletter called **DISSPATCH**.

DISSPATCH contains articles and information that highlight areas of INFOSEC-interest to the DoD and its components. It will include upcoming conferences and courses dealing with INFOSEC, Automated Systems Security Incident Support Team (ASSIST) alerts, reports and bulletin updates, information on INFOSEC policies, plans, programs, products, and architecture. Articles and information are solicited from various INFOSEC experts including you, the reader.

YOUR HELP is needed to get the DISSPATCH out to all personnel associated with or responsible for INFOSEC within the DoD. If you have a question or you and others you know would like to receive this newsletter, please give us the following information: name, organization, address, telephone number, copies desired. Write or call us at: DISA/DISSP/TFED 3701 N. Fairfax Dr. Arlington, VA 22203-1713 ATTN: NEWSLETTER, (703) 696-1897, DSN:226-1897.

* Under the Defense Information Systems Agency, in cooperation with The National Security Agency and chartered by the Office of The Assistant Secretary of Defense.

Don't Keep it a SECRET, spread the word about the Defense Security Institute's

INFORMATION SECURITY ORIENTATION COURSE

Who is the course designed to serve?

Government employees who are:

- Part-time security managers and assistant security managers
- People who need an overview of the information security program
- People who have responsibilities pertaining to classified information
- People who regularly handle classified information
- Document control personnel
- TSCOs and alternates

How long is the course?

- Three days

Where is it held?

- Courses are given at the sponsor's location of choice. We are looking for sponsors for FY 94.

How much does it cost?

- Per diem and travel costs for two instructors.

How can I find out more?

- **Call Course Manager Cheryl Cross at DoDSI, DSN 695-4390, COMM (804) 279-4390. fax: DSN 695-5239, (804) 279-5239**

What is included in the course?

- The classification process
  - Who can originally/derivatively classify
  - Original classification process
  - Derivative classification process
  - Applying theory with practical exercises
- Marking information
  - Markings common to all classified and unclassified sensitive documents
  - Applying theory with practical exercises
- Accountability and control systems
  - TS accountability procedures
  - Secret/Confidential procedures
  - Two-person integrity
  - Classified reproduction procedures
- Custodial responsibilities
  - Security Standard Forms
  - Mailroom
  - End of the day security check
  - Exit/entrance inspection program
  - Courier authorization card
- Safes and locks
  - GSA containers
  - Other types of containers
  - Authorized locks
- Transmission/transportation
  - Transporting
  - Packaging
  - Handcarrying
- Disposal/destruction
  - Who can?
  - When to?
  - Methods
  - Procedures
  - Precautions
- Violations/compromises

You can ... Win with SPIN

The Security Program Improvement Network

Everyone, at some time, identifies a problem and comes up with the right solution. Within the security arena, someone—every day—comes up with that solution. What happens, though, is that the solution is rarely passed on to others who meet the same or a similar type problem.

The Department of Defense recognizes this fact of life and has a new program to help capture and share these solutions with others. It's called the Security Program Improvement Network, "SPIN" for short.

The security pros in the DOD know that getting a job done right is much more than just doing what is required. When one of them finds a better way, you can bet there are many others who want to adopt the idea. SPIN is the link between those with tried-and-true solutions and those still looking for the right answer.

Since SPIN was first announced in the September 1992 issue of the Security Awareness Bulletin, we have received a number of comments. We're looking for a few more ideas and solutions before we go to press with the first generation of contributions.

What Are We Looking For?

Success in getting better results in applying program requirements that others can try is our bottom line. They should be ones that have wide application in your agency or component. They may be about:

- How to operate a program, the procedures you have introduced, or what you've done to motivate security support;
- Your approach to assistance and inspection; how you've established the value of security.
- The equipment you use, the software you have created or applied, how you've overcome a problem inherent in the requirements, etc.
- An article, book, or other publication, or even software you have found particularly helpful in improving your security operation also qualifies for the SPIN program.

Taking Part

How do you share your success and ideas? It's easy.

Just describe the problem or situation, what you did to make improvements, how you did it, what difficulties you had, and how you overcame them.

For ideas you want to "test" with others, just tell what it is, why you think it will help, and how it will work.

For publications and software, give us your assessment of their value and application. You'll need to say where they can be obtained and identify the author and title. If you send software, include a brief description of what it does, how to use it, and any conditions for its release to others.

Be as detailed as need be and include a citation of any related regulations that apply.

If your submission is classified, limit it to no higher than Secret and make sure you've got it correctly portion marked.

Submit your contribution in typed form and (if you can) include a copy on diskette (5.25 or 3.5 inches) in a DOS program.

Please make sure you:

> Include your name, organization, component or company, mailing address, and telephone number (commercial and, where available, DSN numbers).

> Tell us if you want your name, organization or component or company identified in reviewing or publishing your contribution.

> Include any restriction that you know of and the authority on releasing its content to other federal agencies and personnel, to contractors, or to the public.

Send your SPIN communications to:

DOD Security Institute
ATTN: SPIN Coordinator
c/o DGSC
8000 Jeff Davis Highway
Richmond, VA 23297-5091

You Can Host These Courses On-site at your Facility (Industry or Government)

Security Briefers Course (SBC) 5220.13, 2.5 days

Purpose: To improve your effectiveness as a security education briefer. You will receive instruction on how to:

- prepare a briefing plan;
- design and use briefing aids;
- present your briefings in a clear and interesting manner; and
- evaluate live briefings.

As the "Security" in the course title suggests, the briefings must address security requirements, but this is not the emphasis of the course. The course emphasis is on accomplishing the objectives listed above so that you become more skilled and more comfortable at speaking in front of others.

Train-the-Trainer Course (TTT) 5220.13a, 4.5 days

Purpose: To train you to teach the SBC. This workshop, conducted on the 2 days before a scheduled SBC, prepares you to be an instructor for the SBC. You will receive instruction by DoDSI staff on how to:

- use the SBC materials;
- present selected lessons in the SBC;
- facilitate the preparation of briefings;
- conduct practice briefing sessions; and
- evaluate live briefings.

Under DoDSI supervision, you will then spend the next 2.5 days teaching your first SBC.

If you are considering participating in the TTT, it is suggested that you: be responsible for your organization's security briefing program; be an experienced security briefer or a graduate of the SBC; have a need to train others to prepare and present security briefings; and have a working knowledge of security requirements. If you want to learn *how* to brief—choose the SBC.

To host the courses described above, please call Del Carrell, DoDSI at (804) 279-5314 or DSN 695-5314.

These courses are held in succession. The TTT precedes the SBC.

To host the SBC, you must be able to provide:

- ☐ one main classroom for 24 students
- ☐ 3 breakout rooms for 6 students each
- ☐ A-V equipment for all 4 rooms (Overhead projectors, screens, and writing surfaces for each room)
- ☐ At least two of the instructors and preferably more for the TTT.
- ☐ An on-site coordinator
- ☐ Invitations to other security organizations in your area in order to fill a class of 24.

The Department of Defense Security Institute (DoDSI) will:

- ✔ Provide the lead instructor and assume responsibility for the teaching success of the course.
- ✔ If necessary, provide security personnel from other organizations to help teach the course.
- ✔ Provide two full days of training for the instructors prior to starting the course.
- ✔ Provide the instructional materials in sufficient quantities for 24 students.
- ✔ Help the trainers teach the Security Briefers Course.

Here's your chance to sign up for the Security Briefers Course!

April, 6-8, 1993 **Richmond, VA**

DoDSI Resident Courses

POC: MS. DEL CARRELL
DoD Security Institute
c/o DGSC
Richmond, VA 23297-5091
(804) 279-5314, (DSN) 695-5314

April 27-29, 1993 **Downey, CA**

Greater Los Angeles ISAC

POC: MS. RANDI HENRICKSON
Rockwell International Corporation
12214 Lakewood Blvd.
Downey, CA 90241
(310) 797-4065

May 5-7, 1993 **Brooklyn, MN**

National Classification Management Society - Minneapolis / St. Paul Chapter

POC: MR. DENNIS TKACH
Alliant Tech System
7225 Northland Drive
Brooklyn, MN 55428
(612) 536-4595

May 12-14, 1993 **Albuquerque, NM**

ISAC - New Mexico

POC: MS. SHIRLEY SHOBE
Defense Investigative Service (S42AQ)
P.O. Box 18028
Kirtland AFB, NM 87185-0028
(505) 846-1814, (DSN) 246-1787

May 18-20, 1993 **Los Angeles, CA**

Greater Los Angeles ISAC

POC: MS. RANDI HENRICKSON
Rockwell International Corporation
12214 Lakewood Blvd.
Downey, CA 90241
(310) 797-4065

May 19-21, 1993 **White Sands Missile Range, NM**

Southwest ISAC

POC: MR. ART MARQUEZ
White Sands Missile Range
White Sands, NM 88002-5041
(505) 678-4502, (DSN) 258-4502

June 23-25, 1993 **Phoenix, AZ**

Phoenix ISAC

POC: MR. ED HYLAND
Defense Investigative Service (S42PX)
201 East Indianola, Suite 360
Phoenix, AZ 85012-2055
(602) 640-2448

July 27-29, 1993 **Richmond, VA**

DoDSI Resident Course

POC: MS. DEL CARRELL
DoD Security Institute
c/o DGSC
Richmond, VA 23297-5091
(804) 279-5314, (DSN) 695-5314

August 4-6, 1993 **Huntsville, AL**

HISAC (Huntsville ISAC)

POC: MS. KATHY PRITCHETT
Defense Investigative Service (V4100)
2300 Lake Park Drive, Suite 250
Smyrna, GA 30080-7606
(404) 432-0826, (DSN) 697-6785

August 9-13, 1993 **Ft. Knox, KY**

US ARMY

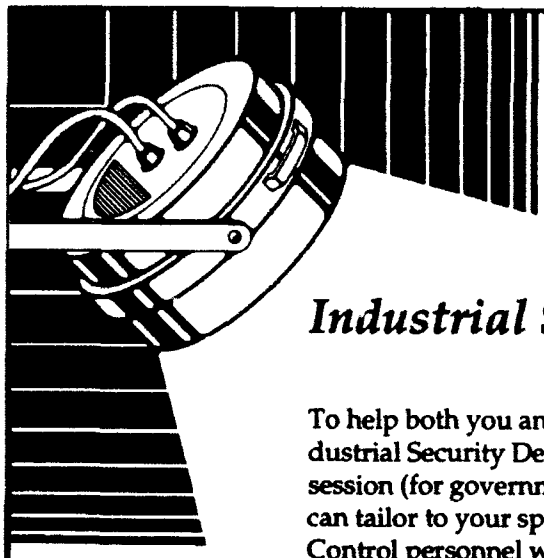
POC: MS. RHONDA MURRAY
US Army Armor Center
Ft. Knox, KY 40121
(DSN) 464-7186

September 20-24, 1993 **Atlanta, GA**

TRISAC

POC: MS. KATHY PRITCHETT
Defense Investigative Service (V4100)
2300 Lake Park Drive, Suite 250
Smyrna, GA 30080-7606
(404) 432-0826, (DSN) 697-6785

Please call the Point of Contact for course specifics and enrollment information.



Industrial Security — Customized

To help both you and the already overworked Industrial Security Rep, the Industrial Security Department faculty at DoDSI now has a one- to two-day training session (for government and industry) that covers industrial security subjects ***you*** can tailor to your specific needs. For example, do you have numerous Document Control personnel who need training in accountability, reproduction, destruction? We can help. ***You*** work with us in the design. ***You*** pick the site; no cost other than travel, food, and lodging for one or two instructors.

For more details about this offer, please call Wayne Lund on (804) 279-3939.

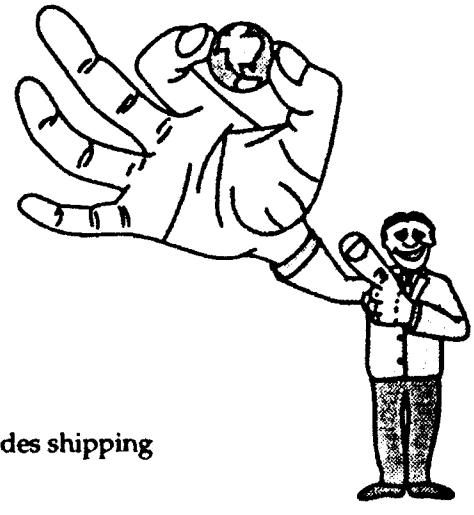
Videos . . .

Briefing the Susceptible Traveler

Date: 1991 Length: 11:44 min. Medium: 1/2"

Order from: Pro Star International Cost $20.00 includes shipping
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178

Summary: A brief-the-briefer video for security managers who need to brief employees traveling outside the U.S. Produced by Northrop Corporation in conjunction with the FBI's Susceptible Traveler Program. Closed captioned for the hearing impaired.



Foreign Travel Briefing — Don't Leave Home Without It

Date: 1991 Length: 7:10 min. Medium: 1/2"

Order from: Pro Star International Cost: $20.00 includes shipping
P.O. Box 21526
Salt Lake City, UT 84121
1-800-775-0761
fax: (801) 943-5178

Summary: Designed to be viewed by the average employee traveling to a foreign country. Produced by Northrop Corporation. Closed captioned for the hearing impaired. These two videos can be ordered as a set for $35.00.

A New Crowd Pleaser at DoDSI!

The **Advanced Industrial Security Management Course** (AISMC) is for defense contractor personnel. This course goes beyond the ever-popular Industrial Security Management Course to emphasize specific requirements and administrative procedures in safeguarding classified defense information for possessing facilities.

Some of the topics to be presented:

- International Aspects
- Independent Research and Development
- STU-III
- AIS Security
- Alarms
- Technology Transfer

Assisting the DoDSI faculty are Department of Defense specialists offering unique insight into particular programs.

We encourage you to sign up for one of the dates offered below during FY 93:

June 15 - 17, 1993
August 31 - September 2, 1993

The prerequisites. To attend the AISMC you:

- ✔ must have been involved with the Defense Industrial Security Program for at least three years.
- ✔ should also have successfully completed the Industrial Security Management Course.

To register, please fill out this page and mail to:

Attn: Registrar
DoD Security Institute
8000 Jefferson Davis Highway, Bldg 33E
Richmond, VA 23297-5091

Your Name Mr./Mrs./Ms._____

Position _____

SSN _____ Telephone _____

Company Name _____

Address _____

_____

Supervisor _____

Course Dates _____

Please provide a copy of the certificate you received for completing the Industrial Security Management Course. If not available, show when and where you completed the course:

Month and year _____

Location _____

If you have questions about enrolling, the Registrar's Office can help you.
Their number is (804) 279-4891.

Interagency OPSEC Support Staff ★★★★★

A new IOSS publication, *Arms Control Treaties: The Threat*, has recently been released to the OPSEC community. This new product, the eighth and final publication in the Treaty Inspections Series, provides an unclassified threat assessment that can be used in preparation for treaty-related on-site inspections. Distribution is authorized to U.S. Government agencies and their supporting contractors. To get a copy of this publication (which is For Official Use Only) write to:

IOSS
Attn: Publications Officer
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405

Video . . .

OPSEC: Protecting Our Edge

Date: 1992 Length: 9 min.

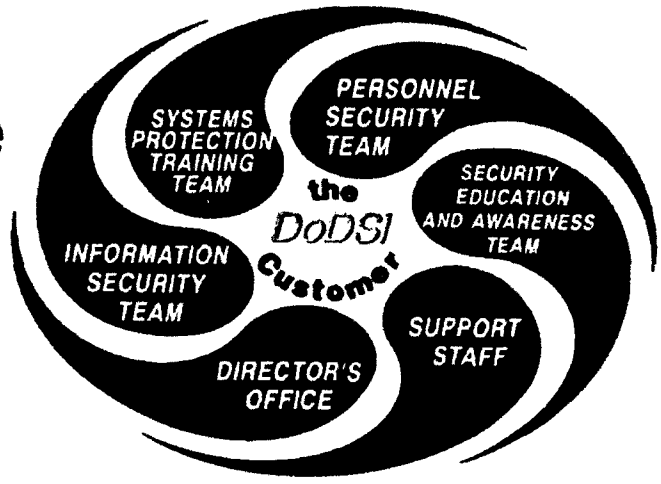
The Interagency OPSEC Support Staff has released a videotape to the OPSEC community. Explains how OPSEC can help protect sensitive technological and economic information from loss to foreign competitors. Produced by the Defense Information Systems Agency. The tape had its "world premier" at the National OPSEC Conference. Video is no cost.

Order from:

Interagency OPSEC Support Staff
Attn: Publications Department
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405

A Change for the Better

The "New" DoDSI?



Several months ago, the Department of Defense Security Institute was the subject of a management study commissioned by Nina Stewart, Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures. When the study results were presented, there was some good news and some that wasn't so good. On the "up" side, the Institute received very high marks on the competence and professionalism of its staff. And based on a survey of Institute customers, internal quality measures, and its own observations, the study team rated the quality of the Institute's products and services as exceptionally high. On the "down" side, the study identified important needs for improvement in certain aspects of productivity and organizational climate. So what did we do? Following the old dictum of government service — "when in doubt, reorganize" — we reorganized.

In this case, though, it wasn't reorganization for reorganization's sake. And it wasn't just a shuffling of people and changing of titles on wiring diagrams. It was a drastic and fundamental change in the way we are organized to do business. And to make sure everyone was *thoroughly* confused — we began two other important efforts to change the way we approach doing business and provide more cost-effective support to DoD's security programs. Let's look at the reorganization first.

Our old structure was a traditional, hierarchical arrangement, with a Director's office, four departments, and eight divisions. Literally overnight, all those elements except the Director's office and the Administrative Services Division (which shrunk to a shadow of its former self) disappeared. The Institute's former supervisors found themselves members of a Support Staff and various working groups, and the rest of the staff and faculty were organized into self managing teams. The result? As close to utter chaos as anything you've ever seen.

Countless hours were spent in meetings, with a common sight being someone rushing out of one meeting to avoid being late for another. All the old lines of authority were gone, and people found themselves making decisions instead of asking questions. "Check with your team" replaced "ask your supervisor," and "we'll figure it out" took the place of "we'd better ask the boss." People who until then had barely exchanged more than a "hello in the hall found themselves depending on each other to get things done. Anxiety? Discomfort? Uncertainty? Stress? You bet. Change is difficult, and this was a radical and sudden change from the sort of work environment all of us had grown up in.

Rather incredibly, in the midst of this turmoil, the people of the Institute continued to do their jobs and provide the expected service to our customers. Resident and field extension courses were conducted as scheduled — including the first public offering of our new Classification Management Course, the prototype of the new Advanced Industrial Security Management Course, and a field extension Special Access Program orientation seminar. Work

continued on our independent study courses, publications, and projects. You'll have to excuse us if we seem awfully proud of the exceptional professionals who made this happen.

Right now, we're clawing our way out of the chaos. The teams are hammering out ways to get their jobs done most effectively. And we're all working on complicated questions of performance measurement, roles and goals, and the like. When we emerge from the fog, here's what you're going to see.

☞ You're going to see an Institute where highly skilled professionals make the decisions instead of having them made for them.

☞ You'll see an organization where every employee has both a say and a stake in how the job gets done and how well.

☞ You'll see a place where every single person who works there has and accepts a personal responsibility for the quality of service we provide to our customers and their security programs.

☞ And you'll see an Institute where most of the time we *used* to spend supervising and administering will be devoted to getting the job done.

What about those two other efforts? The first is the application of Total Quality Management principles to the way we do business. Although the quality of our end products and services is rated as high, we're much less satisfied with our productivity. One way we could raise productivity is to cut quality but, frankly, that idea is completely unacceptable to the Institute's staff and faculty. The management study told us that the hallmark of DODSI is quality. We absolutely refuse to degrade the quality of what we provide to our customers. We think the answer to raising productivity while maintaining quality is to make good use of the concepts of TQM, and we're going to do just that.

☞ We'll be forming process action teams to examine and enhance the effectiveness and efficiency of many of the internal processes we use to do our work.

☞ We'll be consulting with our customers to find ways to smooth bumps in the road of dealing with them.

☞ And we'll be taking a critical look at the tasks and functions we perform every day. When we identify tasks that do not add value to what we deliver to our customers, they're history. For tasks that do add value, we'll make sure that they have maximum effectiveness and minimum resource cost.

The other major change we're making is to install the "marketing concept" as an essential element of our approach to our business. This means doing a thorough, structured analysis of (1) the needs of our customers (and potential customers), (2) our own products, services and capabilities, and (3) the ways we bring our customers and our products together, then using the results to plan how we can best use the Institute's resources to fill the identified needs. Using marketing techniques and tactics will let us make sure that our products and services do the best possible job of filling real needs of our customers, that we make the most productive use of our resources, and that our products and services reach those who need them when they need them.

With all the changes we're making, it would be tempting to start calling this "The New DODSI." But it really isn't. It's the same Institute, changing its ways to bring you the same high quality of products and services, but in smarter, more responsive and more productive ways. We think you're going to like it.

Security Awareness Publications Available From The Institute

Send this form with **mailing label** to:

DoD Security Institute
Attn: Security Education and Awareness Team
c/o Defense General Supply Center
8000 Jefferson Davis Hwy., Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

(TAS) Training Aids for Security Education. June 1992. Catalog of audiovisual and printed material of interest to security educators. Instructions for ordering. . . . . ___

(REC) Recent Espionage Cases: Summaries and Sources. September 1991. Seventy-eight cases, 1975 through 1991. "Thumb-nail" summaries and open-source citations. . . . . ___

(FIT) The Foreign Intelligence Threat to U.S. Defense Industry. By Defense Security Institute staff. January 1991. . . . . ___

(FTB) Foreign Travel Briefing. Script of briefing designed for cleared employees traveling to designated countries. Outlines methods used by hostile intelligence services and precautions against them. (For 14-minute tape/slide briefing, see "Training Aids for Security Education.") . . . . . ___

(CUT) Control of Unclassified Technical Data with Military or Space Application, May 1985. DoD 5230.25-PH. 20-page booklet prepared by the Office of Secretary of Defense explaining the DoD program to limit public disclosure of export-controlled technical data and the special markings for technical documents. . . . . ___

(SAM) Soviet Acquisition of Militarily Significant Western Technology: An Update, September 1985. Western products and technology secrets are being systematically acquired by intricately organized, highly effective collection programs. . . . . ___

DELIVER! Easy-to-follow pamphlet on how to transmit and transport your classified materials. . . . . ___

Terminator VIII Requirements for destruction of classified materials. Contains questions and answers for some common problems and also detailed information on various destruction methods. . . . . ___

Security Awareness Bulletin. Back issues available from the Institute:

(1-90)	Oct 89	Foreign Travel. FOR OFFICIAL USE ONLY.	___
(2-90)	Jan 90	The Case of Randy Miles Jeffries	___
(3-90)	Apr 90	Beyond Compliance – Achieving Excellence in Industrial Security	___
(4-90)	Aug 90	Foreign Intelligence Threat for the 1990s	___
(1-91)	Jan 91	Regional Cooperation for Security Education	___
(2-91)	Sep 91	AIS Security	___
(1-92)	Oct 91	Economic Espionage	___
(2-92)	Feb 92	Self-Inspection Handbook	___
(3-92)	Mar 92	OPSEC	___
(4-92)	Sep 92	What is the Threat and the New Strategy?	___

Individual back issues of the *Security Awareness Bulletin* up through #2-89 are no longer available from the Institute. Reprints of past feature articles have been brought together under a single cover in a publication, *Security Awareness in the 1980s*. Available from the Government Printing Office, stock number 008-047-00394-3. Price is $11.00. To order call (202) 783-3238.